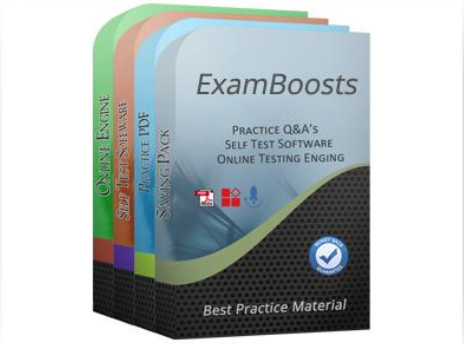
ExamBoosts

TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.examboosts.com/

Reliable & Efficient Test Practice Questions to Satisfy All Candidates

Exam : **NSE4_FGT-6.0**

Title : Fortinet NSE 4 - FortiOS 6.0

Vendor : Fortinet

Version : DEMO

NO.1 Examine the exhibit, which shows the output of a web filtering real time debug.

Why is the site www.bing.com being blocked?

A. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.

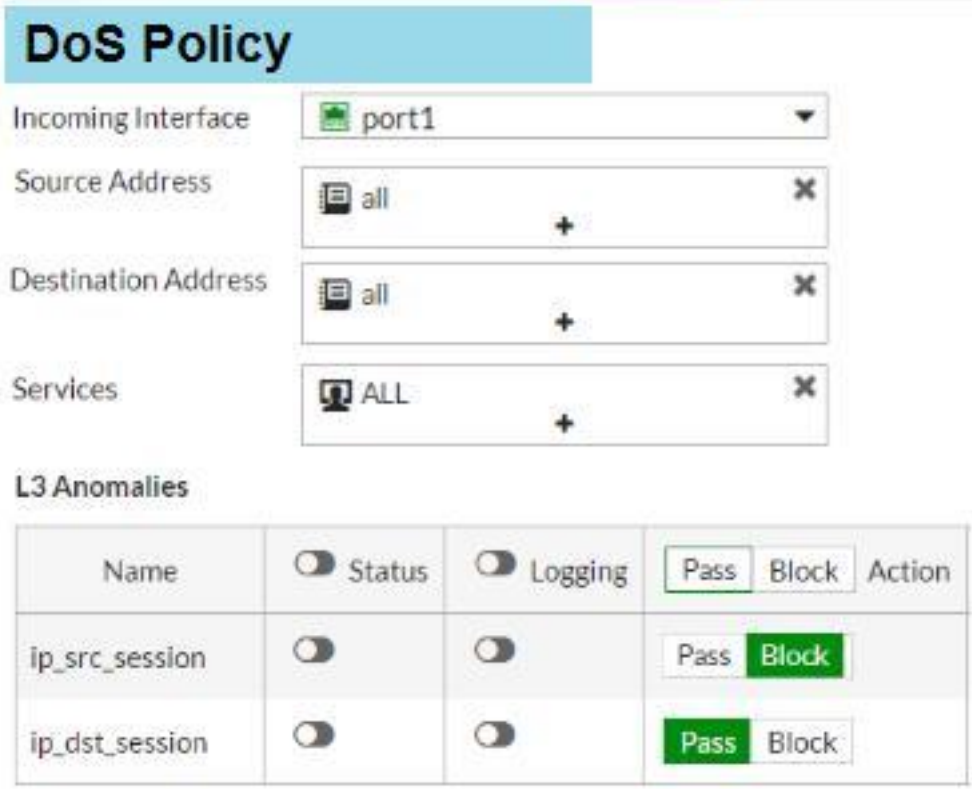
B. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.

C. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.

D. The user has not authenticated with the FortiGate yet.

Answer: C

NO.2 Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. SMTP.Login.Brute.Force

B. ip_src_session

C. Location: server Protocol: SMTP

D. IMAP.Login.brute.Force

Answer: D

NO.3 Which of the following statements about policy-based IPsec tunnels are true? (Choose two.)
A. They require two firewall policies: one for each directions of traffic flow.
B. They support GRE-over-IPsec.
C. They support L2TP-over-IPsec.
D. They can be configured in both NAT/Route and transparent operation modes.
Answer: C,D

NO.4 Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?
A. The CA certificate that signed the web-server certificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The private key of the CA certificate that signed the browser certificate must be installed on the browser.
D. The public key of the web server certificate must be installed on the browser.
Answer: A

NO.5 View the exhibit.

```
date=2018-01-30 time=07:21:49 logid="0316013057" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="root" logtime=1517325709 policyid=1
sessionid=15332 srcip=10.0.1.20 scrport=59538 srcintf="port3" srcintfrole="undefined"
dstip=208.91.112.55 dstport=80 dstintf="port1" dstintfrole="undefined" proto=6
service="HTTP" hostname="lavito.tk" profile="Category-block-and-warning" action="blocked"
reqtype="direct" url="/" sentbyte=140 rcvdbyte=0 direction="outgoing" msg="URL belongs
a category with warnings enabled" method="domain" cat=0 catdesc="Unrated" crscore=30
crlevel="high"
```

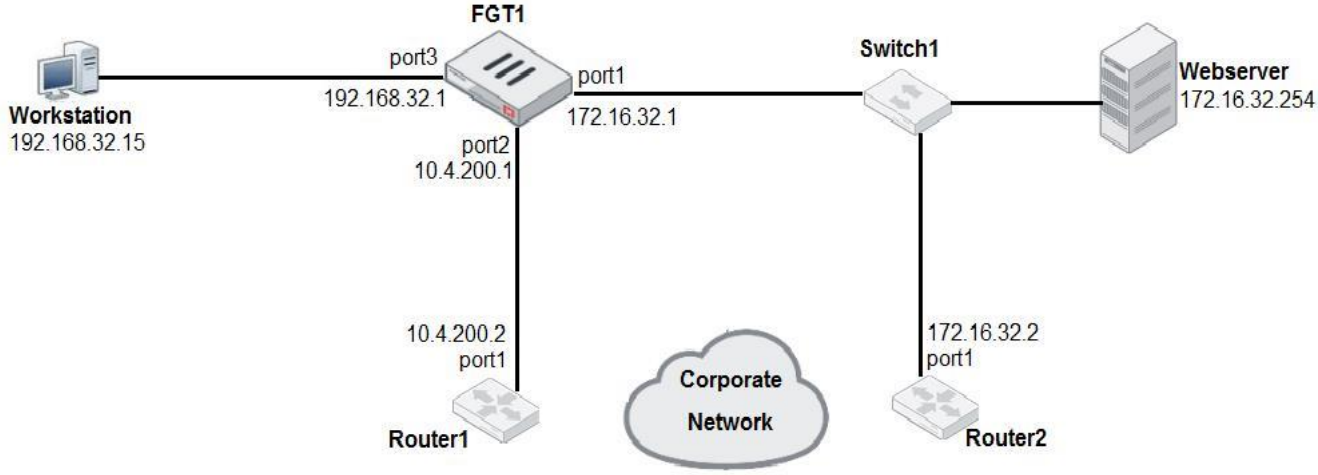
ID	Name	From	To
2	IPS	port1	port3
1	Full_Access	port3	port1
0	Implicit Deny	any	any

What does this raw log indicate? (Choose two.)
A. FortiGate blocked the traffic.
B. 10.0.1.20 is the IP address for lavito.tk.
C. policyid indicates that traffic went through the IPS firewall policy.
D. type indicates that a security event was recorded.
Answer: C,D

NO.6 Which action can be applied to each filter in the application control profile?
A. Block, monitor, warning, and quarantine
B. Allow, monitor, block and learn
C. Allow, monitor, block, and quarantine

D. Allow, block, authenticate, and warning
Answer: C

NO.7 Examine the network diagram shown in the exhibit, then answer the following question:



Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?
A. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
B. 172.16.32.0/24 is directly connected, port1
C. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
D. 10.4.200.0/30 is directly connected, port2
Answer: B

NO.8 Which statements about DNS filter profiles are true? (Choose two.)
A. They can block DNS requests to known botnet command and control servers.
B. They can redirect blocked requests to a specific portal.
C. They can inspect HTTP traffic.
D. They must be applied in firewall policies with SSL inspection enabled.
Answer: A,B

NO.9 What settings must you configure to ensure FortiGate generates logs for web filter activity on a firewall policy called Full Access? (Choose two.)
A. Enable disk logging.
B. Enable a web filter security profile on the Full Access firewall policy.
C. Enable Log Allowed Traffic on the Full Access firewall policy.
D. Enable Event Logging.
Answer: B,C

NO.10 View the certificate shown to the exhibit, and then answer the following question:

Field	Value
Version	V3
Serial Number	98765432
Signature algorithm	SHA256RSA
Issuer	cn=RootCA,o=BridgeAuthority, Inc., c=US
Valid from	Tuesday, October 3, 2016 4:33:37 PM
Valid to	Wednesday, October 2, 2019 5:03:37 PM
Subject	cn=John Doe, o=ABC, Inc.,c=US
Public key	RSA (2048 bits)
Key Usage	keyCertSign
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	CA=True, Path Constraint=None
CRL Distribution Points	URL=http://webserver.abcinc.com/arlcert.crl

The CA issued this certificate to which entity?

A. A bridge CA

B. A root CA

C. A subordinate CA

D. A person

Answer: B